AMENDMENTS TO THE CLAIMS

1. (Currently amended) A system for securely playing a content stream, comprising:

(a) a processor that is arranged to perform actions, including:

(1) selectively encrypting at least a portion of the content stream using a content key;

(2) encrypting the content key using a screener key; and

(3) encrypting the screener key using a public key; and

(b) a player that is arranged to receive the selectively encrypted content stream and encrypted screener key, and to perform actions, including:

(1) decrypting the encrypted screener key using a private key associated with the public key, wherein the public key and the private key are bound to the player such that the public key and the private key are unique to the player;

(2) decrypting the encrypted content key using the screener key; and

(3) decrypting the selectively encrypted content stream using the content key.

2. (Original) The system of claim 1, wherein the player is arranged to perform actions, further comprising, employing a user identity to enable access to the encrypted screener key.

3. (Previously presented) The system of claim 1, wherein the player further comprises:

(a) an authentication module that is arranged to perform actions, including:

receiving a user identity;

authenticating the received user identity;

determining an authorization associated with the user identity; and

if the user identity is authorized to access the encrypted screener key, enabling the encrypted screener key to be retrieved.

4. (Original) The system of claim 1, wherein the encrypted screener key resides on at least one of a smart card, PCMCIA card, memory stick, DVD, CD, tape, and a floppy disc.

5. (Original) The system of claim 1, wherein selectively encrypting at least a portion of the content stream further comprises encrypting at least a portion of at least one of a video elementary stream (ES), audio ES, intra-frames (I-frames), forward predicted frames (P-frames), and bi-directional predicted frames (B-frames).

6. (Original) The system of claim 1, wherein selectively encrypting at least a portion of the content stream further comprises employing another content key to encrypt at least another portion of the content stream.

7. (Original) The system of claim 1, wherein selectively encrypting at least a portion of the content stream further comprises rotating through a plurality of content keys, each of which is employed to selectively encrypt a different portion of the content stream.

8. (Previously presented) An apparatus for securely playing content, comprising:

(a) a loader configured to receive a screener key associated with a selectively encrypted content stream, wherein the screener key is encrypted using a public key that is bound to the apparatus such that the public key is unique to the apparatus; and

(b) a decryption engine, coupled to the loader, that is configured to perform actions, including:

(1) receiving the selectively encrypted content stream;

(2) employing the loader to retrieve the screener key;

(3) decrypting the screener key using a private key associated with the public key, wherein the private key is constrained to the apparatus; and

(4) employing the screener key to decrypt a content key, wherein the content key enables decryption of the selectively encrypted content stream.

9. (Original) The apparatus of claim 8, wherein the loader is configured to perform actions, further comprising:

(a) receiving a request for access to the screener key from the decryption engine;

(b) requesting authorization to provide access, from an authentication module; and

(c) if authorization is received, providing the encrypted screener key to the decryption engine.

10. (Original) The apparatus of claim 8, wherein the loader is further configured to store another screener key on a screener key module.

11. (Original) The apparatus of claim 10, wherein the screener key module comprises at least one of a smart card, PCMCIA card, memory stick, DVD, CD, tape, and a floppy disc.

12. (Original) The apparatus of claim 8, wherein the private key and public key associated with the apparatus are generated by a Federal Information Processing Standard (FIPS) level 4 device.

13. (Original) The apparatus of claim 8, further comprising a tamper agent configured to monitor for an unauthorized action and, if an unauthorized action is detected, to provide a response to the unauthorized action.

14. (Original) The apparatus of claim 13, wherein the response to the unauthorized action further comprises at least one of erasing the selectively encrypted content stream, locking the apparatus from an operation, erasing the private key, erasing the screener key, and reporting the unauthorized action.

15. (Previously presented) A method for creating secure content for use in a player, the method comprising:

(a) selectively encrypting at least a portion of a content stream using a content key;

(b) generating a key package comprising the content key;

(c) encrypting the key package using a screener key;

(d) encrypting the screener key employing a public key bound to the player such that the public key is unique to the player;

(e) embedding the encrypted key package into the selectively encrypted content stream.

16. (Original) The method of claim 15, further comprising, copying the selectively encrypted content stream including the embedded key package onto a content media.

17. (Original) The method of claim 16, wherein the content media further comprises at least one of a DVD, high definition DVD, Video Compact Disc (VCD), Super VCD (SVCD), Super Audio CD (SACD), Dynamic Digital Sound (DDS) media, Read/Write DVD, and a CD-Recordable (CD-R).

18. (Original) The method of claim 15, wherein the content key is generated employing a encryption/decryption algorithm comprising at least one of Advanced Encryption Standard (AES), RSA, International Data Encryption Algorithm (IDEA), and Data Encryption Standard (DES) algorithm.

19. (Original) The method of claim 15, wherein the key package further comprises at least one of synchronization information that indicates a relationship between the content key and the selectively encrypted content stream, and a content identifier associated with the content stream.

20. (Original) The method of claim 15, wherein the key package further comprises a content identifier associated with the content stream, wherein the content identifier remains unencrypted.

21. (Original) The method of claim 15, further comprising, storing the encrypted screener key in a screener key module, wherein the screener key module is removable from the player.

22. (Original) The method of claim 15, wherein the screener key module further comprises at least one of a content identifier associated with the selectively encrypted content stream, an access constraint, and a fulfillment right.

23. (Original) The method of claim 15, wherein selectively encrypting at least a portion of a content stream further comprises selecting for encryption at least a portion of at least one of a video elementary stream (ES), audio ES, intra-frames (I-frames), forward predicted frames (P-frames), and bi-directional predicted frames (B-frames).

24. (Original) The method of claim 15, wherein the screener key is generated employing a encryption/decryption algorithm comprising at least one of an Advanced Encryption Standard (AES), RSA, International Data Encryption Algorithm (IDEA), Skipjack, RC4, and a Data Encryption Standard (DES) algorithm.

25. (Original) The method of claim 15, wherein selectively encrypting at least a portion of a content stream further comprises partitioning the content stream into content units.

26. (Previously presented) A method for securely playing a content stream, comprising:

(a) receiving the content stream, wherein the content stream comprises at least one selectively encrypted content unit;

(b) receiving a key package, wherein the key package is encrypted using a screener key;

(c) retrieving the screener key, wherein the retrieved screener key is encrypted using a public key;

(d) decrypting the retrieved screener key using a private key associated with the public key wherein the private key is constrained to a content stream player such that the public key and the private key are unique to the content stream player;

(e) decrypting the key package using the decrypted screener key; and

(f) decrypting at least one selectively encrypted content unit using the decrypted content key.

27. (Canceled)

28. (Currently amended) The method of claim 26, wherein the decrypted content unit comprises a compressed content unit, further comprising, decompressing the ~~decrypted~~ compressed content unit.

29. (Original) The method of claim 26, wherein retrieving the screener key further comprises, determining an authorization to retrieve the screener key.

30. (Original) The method of claim 26, wherein the selectively encrypted content unit further comprises at least a portion of at least one of a video elementary stream (ES), audio ES, intra-frames (I-frames), forward predicted frames (P-frames), and bidirectional predicted frames (B-frames).

31. (Original) The method of claim 26, wherein the screener key is generated employing a encryption/decryption algorithm comprising at least one of an Advanced Encryption Standard (AES), RSA, International Data Encryption Algorithm (IDEA), Skipjack, RC4, and a Data Encryption Standard (DES) algorithm.

32. (Previously presented) A computer-readable medium encoded with a data structure for use in securing content, the data structure comprising:

a first data field comprising at least one selectively encrypted content unit from a content stream;

a second data field comprising a key package, wherein the key package comprises at least one content key for decrypting the at least one selectively encrypted content unit, and a content identifier associated with the content stream, wherein the at least one content key is encrypted using a screener key, the screener key being encrypted using a public key bound to a targeted player such that the public key is unique to the targeted player.

33. (Original) The computer-readable medium of claim 32, wherein the key package further comprises an access constraint associated with the content stream.

34. (Canceled)

35. (Original) The computer-readable medium of claim 32, wherein the second data field is interspersed between at least two content units.

36. (Original) The computer-readable medium of claim 32, wherein the content key is generated employing a encryption/decryption algorithm comprising at least one of Advanced Encryption Standard (AES), RSA, International Data Encryption Algorithm (IDEA), and Data Encryption Standard (DES) algorithm.

37. (Original) The computer-readable medium of claim 32, wherein the key package further comprises synchronization information that indicates a relationship between at least one content key and the selectively encrypted content unit.

38. (Original) The computer-readable medium of claim 32, wherein the selectively encrypted content unit further comprises at least a portion of at least one of a video elementary stream (ES), audio ES, intra-frames (I-frames), forward predicted frames (P-frames), and bi-directional predicted frames (B-frames).

39. (Original) The computer-readable medium of claim 32, wherein the content stream further comprises a plurality of content units, at least one content unit being of a different length.

40. (Previously presented) The system of claim 1, wherein the processor is arranged to perform further actions, including:

creating a key package that includes the encrypted content key; and

embedding the key package into the content stream.